



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,503	11/02/2000	David J. Wetherall	0016.0005US1	8089
29127	7590	02/28/2008		
HOUSTON ELISEEVA 4 MILITIA DRIVE, SUITE 4 LEXINGTON, MA 02421			EXAMINER BIAGINI, CHRISTOPHER D	
			ART UNIT 2142	PAPER NUMBER
			MAIL DATE 02/28/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/706,503

Applicant(s)

WETHERALL ET AL.

Examiner

CHRISTOPHER D. BIAGINI

Art Unit

2142

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 December 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3,5-14,16,18-27,29,31-39,42-48 and 51-58 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3,5-14,16,18-27,29,31-39,42-48 and 51-58 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed December 6, 2007 have been fully considered but they are not persuasive.
2. Applicant argues that the Poletto application "merely provides that the ratio of incoming to outgoing packets is kept," and that Poletto does not teach or suggest "keeping the differential characteristics between request packets routed out of the network domain, and response packets routed into the domain" (emphasis in original). The examiner respectfully disagrees. The cited passage of Poletto describes keeping the ratio of packets sent between a web browser and a web server, which, by definition, are request packets and response packets. Furthermore, in the paragraph which spans pages 15 and 16 of the Poletto application, Poletto explicitly indicates that the statistics are kept to determine when the servers "are too overloaded to acknowledge the *requests*" (emphasis added). Thus, Poletto provides for keeping track of differential characteristics as required by the claim, and indeed for the very same reason as the instant invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1, 3, 5-14, 16, 18-27, 29, 31-39, 42-48, and 51-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (US PG PUB 2002/0032871, hereinafter "Malan") in view of Poletto et al. (US PG PUB 2002/0032880, hereinafter "Poletto").

2. Regarding claim 1, Malan shows:

- a. a first network domain which is a local area network (comprising the LAN containing DoS source element 17; see [0059] and note that the ISP-2 network is structured in the same manner as ISP-1);
- b. a first routing device at a boundary between the first network domain and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric (collector 20d, see Fig. 7);
- c. a monitor/regulator (collector 20d and controller 24b, see Fig. 7), either integrally disposed in said first routing device (see [0087]) or coupled to the first routing device (see Fig. 7) to monitor the network traffic routed by said first routing device by analyzing flow records (see [0066] and [0071]), describing traffic conversation as indicated by a combination of source and destination addresses (see [0071]), received from the routing device, the monitor/regulator determining if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack in which the undesirable network traffic is launched against a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the first network domain (see p. 8 as scanned of provisional application No. 60/231,481, to which Malan claims benefit, which

Art Unit: 2142

describes the detection of a denial of service attack within the attacker's originating network/source network).

3. Malan does not show wherein said monitor makes said determination based on differential characteristics of network traffic routed out of said first network domain relative to network traffic routed into said first network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

4. Poletto shows making a determination that a network domain is sourcing undesirable network traffic based on differential characteristics of network traffic routed out of a domain relative to network traffic routed into the domain, and aggregating said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain (see pages 15-16 of provisional application No. 60/230,759, to which Poletto claims benefit).

5. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan to use differential characteristics to determine whether network traffic is undesirable as taught by Poletto in order to provide an additional method of detecting denial-of-service attacks (see Poletto, [0054]).

6. Regarding claim 14, it is a method claim corresponding to apparatus claim 1, and is rejected for the same reasons.

Art Unit: 2142

7. Regarding claim 27, it is an apparatus claim directed to a processor and a storage medium including instructions for performing the method of claim 14, and is rejected for the same reasons.

8. Regarding claim 58, it is an apparatus claim containing limitations directed to a network domain, a routing device, and a monitor/regulator as addressed in claim 1 above. However, claim 58 includes the additional limitations of (a) the monitor/regulator generating statistics concerning destination addresses to determine whether the network domain is sourcing the undesirable traffic and (b) the monitor/regulator instructing the routing device to lower a priority of the undesirable network traffic and/or slow the undesirable network traffic. It is noted that Malan teaches these additional features. Malan teaches generating statistics concerning destination addresses to determine whether the network domain is sourcing the undesirable traffic (pars. 70-71). Malan teaches a monitor/regulator that instructs the routing device to lower a priority of the undesirable network traffic and/or slow the undesirable network traffic (60/231,481 pp. 10-11 as scanned, pp. 12-13 as labeled - describing how StormBreaker slows attack traffic to zero; Malan par. 79 showing CAR limiters).

9. Regarding claim(s) 3, 16, 29, 42, 51, Malan further teaches aggregated statistics of traffic data, par. 71.

10. Regarding claim(s) 5, 9, 13, 18, 22, 26, 31, 35, 39, Malan further teaches stopping undesirable traffic being sourced, par. 79.

Art Unit: 2142

11. Regarding claim(s) 6, 10, 19, 23, 32, 36, Malan further teaches a second routing device or network domain through which undesirable traffic is determined as "other router systems", par. 61 and 71.
12. Regarding claim(s) 7-8, 11-12, 20-21, 24-25, 33-34, 37-38, Malan further teaches detecting undesirable traffic between routers as "source ports", par. 71.
13. Regarding claim(s) 43, 52, Malan further teaches determining if sourcing of undesirable traffic/flow based on statistics such as packet lengths, par. 70.
14. Regarding claim(s) 45, 54, Malan further teaches determining if sourcing of undesirable traffic/flow based on statistics such as TCP SYN and FIN packets, par. 83.
15. Regarding claim(s) 46-47, 55-56, Malan further teaches slowing or lowering priority of traffic(60/231,481 pp. 10-11 as scanned, pp. 12-13 as labeled- describing how StormBreaker slows attack traffic to zero; Malan par. 79 showing CAR limiters).
16. Regarding claim(s) 48, 57, Malan further teaches priority levels as groups/categories, par. 68, 70.

Art Unit: 2142

17. Regarding claim 44, 53, the Malan in view of Poletto teaches the method of the preceding claims, but does not explicitly disclose all the details relating to specific types of statistic such as TTL. However, Official Notice is taken that details relating to specific types of statistics is well known in the art to insure a complete data set. It would have been obvious to one of ordinary skill in the art at the time of the application's invention to provide details relating to specific types of statistics to obtain the advantages of having a complete data set. By the above rationale, the claim is rejected.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER D. BIAGINI whose telephone number is (571)272-9743. The examiner can normally be reached on weekdays from 8:30 AM to 5:00 PM..

Art Unit: 2142

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher Biagini
(571) 272-9743



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER